

### REMARKS

Claims 1, 4-14, 16-23, and 26-28 remain pending in the present application. In view of the following remark, Assignee respectfully requests allowance of these claims.

#### **I. Claims 1-29 are not obvious in view of Rockwell and Bentley**

Claims 1-29 presently stand rejected under 35 U.S.C. § 103(a) as being obvious over Rockwell et. al. (U.S. Patent Publ. No. 2003/0027550) in view of Bentley (U.S. Patent No. 6,934,298). For a combination of references to render a claim unpatentable, each claim limitation must be disclosed by the combination of references.

##### **a. Claim 1**

Claim 1 is not obvious in view of Rockwell and Bentley. In combination with other limitations, claim 1 includes the limitations "dynamically identifying a plurality of wireless network sensors in a selected network region," and "selecting for each of the wireless network sensors in the plurality a designation of primary or secondary with respect to the selected network region." In contrast to claim 1, neither Rockwell nor Bentley disclose dynamically identifying wireless sensors in a network region nor do they produce distributed intelligence for wireless intrusion detection as implicated by primary and secondary sensors.

It is apparent that the Office Action has made numerous errors in interpreting the claims and the references. In support of the position that Rockwell shows "dynamically identifying a plurality of wireless network sensors in a selected network region" the Office Action states:

Consequently, the Examiner has interpreted Rockwell to 'dynamically' identify problematic situation when events occur. In simplicity, a 'fault' within the said

MNP, occurs at different locales; therefore, the said system must identify those events, wherein the process is performed dynamically.

This reading displays a complete and utter misunderstanding of the claim element. Whether or not Rockwell "dynamically identif[ies] problematic situations when events occur" is completely irrelevant to the claimed limitation, and is at best a questionable conclusion from the disclosure of Rockwell. The claim limitation at issue reads "dynamically identifying a plurality of wireless network sensors in a selected network region." Assignee respectfully asserts that "dynamically identifying problematic situations" has absolutely no relationship whatsoever to "dynamically identifying...wireless sensors." Whereas "wireless sensors" are clearly hardware devices, "problematic situations" are merely potentially harmful traffic patterns identified within the network traffic.

Moreover, upon reading the rest of the claim, one of ordinary skill in the art should understand that these "wireless sensors" would never be interpreted to be "problematic situations," because the wireless sensors operate in conjunction with a collection agent for collecting information from the wireless network. The data these network sensors collect is used in determining so-called "problematic situations." Therefore, one of ordinary skill in the art should understand that the network sensors themselves are quite beneficial to the security of the network, and are absolutely not "problematic situations." To interpret otherwise is a complete failure to understand the claim, and a failure to understand the previously presented arguments. Given the above, it is abundantly clear that the first and second rejections of this claim were wholly improper and should be immediately withdrawn.

The Office Action further reasons that "Rockwell discloses the use of security data, wherein the Examiner has interpreted as 'scan data'." While these terms may appear facially

equivalent, they are in fact, quite different. Scan data is data that is collected using the network sensors. The sensors can operate to collect wireless traffic in a wireless network region. At various intervals, a collection agent can pull all of the collected wireless traffic to a central repository, whereby an intrusion detection or intrusion prevention system can analyze the data for intrusion or other potentially malicious or unwanted patterns. In contrast, the term "security data" is typically used to describe known security risks. The distributed nature of the collection of the scan data can reduce the processing power required to detect intrusion events. Moreover, the identification of network sensors as primary and secondary enables security logic to avoid inspecting the same traffic twice (e.g., a primary network sensor may receive the traffic, and one or more secondary sensors may receive the same traffic). Thus, the present claims represent a significant advantage over the Rockwell reference in the ability to analyze wireless traffic more efficiently.

Moreover, as should be ascertained from the description above, "secondary sensors" are not equivalent to the "backup access points" disclosed in Bentley. The secondary access points recited in claim 1 operate to collect network traffic. They do not operate to provide a backup access point in case of failure of a primary access point, as disclosed by Bentley. Bentley is directed to a method for providing a standby access point which becomes active **only** upon sensing that an active access point has failed (i.e., backup). In contrast, the access points of claim are used secondarily for data collection. Thus, these access points of claim 1 may be fully operational to transmit network data even though some may be designated secondary for purposes of data collection for the collection agent. One of ordinary skill in the art would understand that the terms backup and secondary, as used in this context are NOT synonymous.

Assignee respectfully asserts that this would be readily apparent to those of ordinary skill in the art, and the rejection should be withdrawn immediately.

Assignee reiterates its traverse of the combination of the Rockwell and Bentley references. Rockwell is only tangentially related to wireless applications in that it provides wireless access to airplane passengers. However, the primary disclosure of Bentley concerns providing network security an airplane network (and because of the remoteness of this roaming network, for all practical purposes, it is a wired network security solution as opposed to a wireless network security solution). Bentley, on the other hand, is entirely related to providing backup wireless network components in case of failure of the active wireless network components. There is absolutely no security aspect to the backup and primary designation of these access points. Moreover, the Office Action has provided no reasonable motivation to combine these references. Rockwell makes no disclosure that a backup network components would even be desirable. Assignee respectfully asserts that such a combination is unwarranted by the disclosures of these references themselves.

b. Claims 2-23

Assignee respectfully urges the Examiner to thoroughly review Assignee's previous response with respect to claims 2-23. These claims highlight exactly how irrelevant the current references are to the claimed invention. Assignee's previous response cites myriad reasons why neither Rockwell nor Bentley disclose the limitations cited by many (if not all) of the dependent claims. Assignee respectfully asserts that it is apparent that none of these reasons have been adequately considered in view of the maintenance of the current rejection.

Moreover, because independent claim 1 is allowable over the cited references, claims 2-23 (which depend from claim 1) are allowable for the reason that these claims include all of the limitations of claim 1. Thus, Assignee respectfully asserts that these claims are in condition for allowance.

c. Claim 24

Claim 24 is not obvious in view of Rockwell and Bentley. In combination with other limitations, claim 24 includes the limitation "dynamically identifying a plurality of wireless network sensors in a selected network region," and "selecting for each of the wireless network sensors in the plurality a designation of primary or secondary with respect to the selected network region." In contrast to claim 24, neither Rockwell nor Bentley disclose dynamically identifying wireless sensors in a network region.

It is apparent that the Office Action has made numerous errors in interpreting the claims and the references. In support of the position that Rockwell shows "dynamically identifying a plurality of wireless network sensors in a selected network region" the Office Action states:

Consequently, the Examiner has interpreted Rockwell to "dynamically" identify problematic situation when events occur. In simplicity, a "fault" within the said MNP, occurs at different locales; therefore, the said system must identify those events, wherein the process is performed dynamically.

This reading displays a complete and utter misunderstanding of the claim element. Whether or not Rockwell "dynamically identif[ies] problematic situations when events occur" is completely inapposite to the claimed limitation, and is at best a questionable conclusion from the disclosure of Rockwell. The claim limitation at issue reads "dynamically identifying a plurality of wireless network sensors in a selected network region." Assignee respectfully asserts that "dynamically identifying problematic situations" has absolutely no relationship whatsoever to "dynamically

identifying...wireless sensors.” Whereas “wireless sensors” are clearly hardware devices, “problematic situations” are merely potentially harmful traffic patterns identified within the network traffic.

Moreover, upon reading the rest of the claim, one of ordinary skilled in the art should understand that these wireless sensors would never be interpreted to be “problematic situations,” because the wireless sensors operate in conjunction with a collection agent for collecting information from the wireless network. The data these network sensors collect is used in determining so-called “problematic situations.” Therefore, one of ordinary skill in the art should understand that the network sensors themselves are quite beneficial to the security of the network, and are absolutely not “problematic situations.” To interpret otherwise is a complete failure to understand the claim, or to understand the previously presented arguments. Given the above, it is abundantly clear that the first and second rejections of this claim were wholly improper and should be immediately withdrawn.

The Office Action further reasons that “Rockwell discloses the use of security data, wherein the Examiner has interpreted as ‘scan data’.” While these terms may appear facially equivalent, they are in fact, quite different. Scan data is data that is collected using the network sensors. The sensors can operate to collect wireless traffic in a wireless network region. At various intervals, a collection agent can pull all of the collected wireless traffic to a central repository, whereby an intrusion detection or intrusion prevention system can analyze the data for intrusion or other potentially malicious or unwanted patterns. In contrast, the term “security data” is typically used to describe known security risks. The distributed nature of the collection of the scan data can reduce the processing power required to detect intrusion events. Moreover,

the identification of network sensors as primary and secondary enables security logic to avoid inspecting the same traffic twice (e.g., a primary network sensor may receive the traffic, and one or more secondary sensors may receive the same traffic). Thus, the present claims represent a significant advantage over the Rockwell reference in the ability to analyze wireless traffic more efficiently.

Moreover, as should be ascertained from the description above, "secondary sensors" are not equivalent to the "backup access points" disclosed in Bentley. The secondary access points recited in claim 1 operate to collect network traffic. They do not operate to provide a backup access point in case of failure of a primary access point, as disclosed by Bentley. Bentley is directed to a method for providing a standby access point which becomes active **only** upon sensing that an active access point has failed (i.e., backup). In contrast, the access points of claim 1 are used secondarily for data collection. Thus, these access points of claim 1 may be fully operational to transmit network data even though some may be designated secondary for purposes of data collection for the collection agent. One of ordinary skill in the art would understand that the terms backup and secondary, as used in this context are NOT synonymous. Assignee respectfully asserts that this would be readily apparent to those of ordinary skill in the art, and the rejection should be withdrawn immediately.

Assignee reiterates its traverse of the combination of the Rockwell and Bentley references. Rockwell is only tangentially related to wireless applications in that it provides wireless access to airplane passengers. However, the primary disclosure of Bentley concerns providing network security an airplane network (and because of the remoteness of this roaming network, for all practical purposes, it is a wired network security solution as opposed to a

wireless network security solution). Bentley, on the other hand, is entirely related to providing backup wireless network components in case of failure of the active wireless network components. There is absolutely no security aspect to the backup and primary designation of these access points. Moreover, the Office Action has provided no reasonable motivation to combine these references. Rockwell makes no disclosure that a backup network components would even be desirable. Assignee respectfully asserts that such a combination is unwarranted by the disclosures of these references themselves.

d. Claim 25

Claim 25 is not obvious in view of Rockwell and Bentley. In combination with other limitations, claim 25 includes the limitation "**means for broadcasting a message to one or more wireless sensors, for receiving acknowledgments from the one or more wireless sensors, for determining whether each of the one or more wireless sensors is within the selected network region, and for each wireless network sensor determined within the selected network region, storing an identifier of that wireless network sensor in the storing means.**" In contrast to claim 25, neither Rockwell nor Bentley disclose identifying wireless sensors in a network region.

Rockwell is directed to a security manager for an airplane cabin wherein the access points for passengers aboard the plane can be wireless access points. Assignee respectfully asserts that there is nothing within the text of Rockwell that discloses that the system performs any identification of wireless sensors. In fact, the secured nature of an airplane would typically indicate that there are no new access points are being added or subtracted from the system. Moreover, the controlled and confined nature of an airplane cabin as disclosed by Rockwell



typically indicates that there would be no need for the backup wireless access points of Bentley. Thus, Assignee respectfully asserts that this reference teaches away from providing primary and secondary access points because of the confined nature of the contemplated network.

Furthermore, Rockwell teaches a centralized collection process as implicated by the control subsystem and airborne security manager (FIG. 1; ref. 26 and 34). As such it is unclear why Rockwell would be improved by providing a distributed primary and secondary collection system aboard an airplane. Thus, there is no motivation to combine this reference apart from motivation found in another reference.

Assignee further notes that because of the mobile and remote nature of the airplane (35,000 feet above the ground) that traditional network security methods apply to the networks of Rockwell, and there is no incentive to provide a collection agent to collect scan data from each of the primary wireless network sensors as required by claim 25. Assignee respectfully asserts that the collection agent of claim 25 is specifically recited as providing scan data ("receiving scan data for the selected network region from the collection agent..."). In stark contrast, Rockwell discloses that the Airborne Security Manager is merely "responsible for enforcing security policy" responsive to intrusion events (see, e.g., ¶22). Assignee respectfully asserts that this is not providing scan data.

Bentley is directed to a method for providing a standby access point which **ONLY** becomes active upon sensing that an active access point has failed. However, Assignee respectfully asserts that the secondary access points as claimed are active and are used for secondary data collection. Thus, these access points of claim 25 can be fully operational to transmit network data even though some may be designated secondary for purposes of data

collection for the collection agent. Thus, Assignee respectfully asserts that the primary/backup designation of Bentley is completely irrelevant to the current claims, and that the rejection should be withdrawn immediately.

Moreover, Bentley mention neither data collection nor wireless security. Thus, Bentley provides no motivation for a combination with Rockwell. Likewise, Rockwell makes no disclosure that a backup network components might be desirable. And, the Office Action has provided no reasonable motivation to combine these references. Therefore, Assignee respectfully asserts that the combination of Rockwell and Bentley is unwarranted.

e. Claim 26

Claim 26 is not obvious in view of Rockwell and Bentley. In combination with other limitations, claim 26 includes the limitations that the system processor include "processing elements programmed or adapted to: broadcast a message to the plurality of wireless network sensors via the communication interface;...receive acknowledgments from the plurality wireless network sensors;...determine whether each wireless network sensor in the plurality is within the selected network region." In contrast to claim 26, neither Rockwell nor Bentley disclose identifying wireless sensors in a network region from a centralized management location.

Rockwell is directed to a security manager for an airplane cabin wherein the access points for passengers aboard the plane can be wireless access points. Assignee respectfully asserts that there is nothing within the text of Rockwell that discloses that the system performs a dynamic identification of wireless sensors. In fact, the secured nature of an airplane would typically indicate that there are no new access points are being added or subtracted from the system. Moreover, the controlled and confined nature of an airplane cabin as disclosed by Rockwell

typically indicates that there would be no need for the backup wireless access points of Bentley. Thus, Assignee respectfully asserts that this reference teaches away from providing primary and secondary access points because of the confined nature of the contemplated network.

Assignee further notes that because of the mobile and remote nature of the airplane (35,000 feet above the ground) that traditional network security methods apply to the networks of Rockwell, and there is no incentive to provide a collection agent to collect scan data from each of the primary wireless network sensors as required by claim 26. Assignee respectfully asserts that the collection agent of claim 26 is specifically recited as providing scan data ("receive scan data for the selected network region from the collection agent..."). In stark contrast, Rockwell discloses that the Airborne Security Manager is merely "responsible for enforcing security policy" responsive to intrusion events (see, e.g., ¶22). Assignee respectfully asserts that this is not providing scan data.

Bentley is directed to a method for providing a standby access point which becomes active only upon sensing that an active access point has failed. However, Assignee respectfully asserts that there is nothing within claim 26 that refers to the secondary access point being an "inactive" access point only used during failure of the primary access point. In contrast, these access points are used secondarily for data collection. Thus, these access points of claim 26 may be fully operational to transmit network data even though some may be designated secondary for purposes of data collection for the collection agent. Thus, Assignee is unclear what application Bentley has to the current claims. Bentley does not mention data collection, nor does it mention wireless security. There is nothing within claim 26 which indicates that the secondary sensing device is only operable upon the primary sensor failing, as disclosed by Bentley.

Applicant respectfully questions the motivation to combine Rockwell with Bentley. Rockwell is only remotely related to wireless applications in that it would like to be able to provide wireless access to airplane passengers, however, it is primarily concerned with providing network security to other passengers (and because of the remoteness of this roaming network, for all practical purposes, it is a wired network security solution as opposed to a wireless network security solution). Bentley, on the other hand, is entirely related to providing backup wireless network components in case of failure of the active wireless network components. However, there is no security aspect to the primary and secondary designation of these access points. Furthermore, Bentley is a completely distributed system whereby each access point determines whether it is active or inactive, whereas the system of claim 26 is a centralized monitoring and management system as should be inherently recognized from the terms of the claim itself. Moreover, the Office Action has provided no reasonable motivation to combine these references, such as the unreliability of an airborne wireless access point. Rockwell makes no disclosure that a backup network components would even be desirable. Assignee respectfully asserts that such a combination is unwarranted by the disclosures of these references themselves.

f. Claims 27-29

Because independent claim 1 is allowable over the cited references, claims 27-29 (which depend from claim 26) are allowable for the reason that they include all of the limitations of claim 26. Thus, Assignee respectfully asserts that these claims are in condition for allowance.

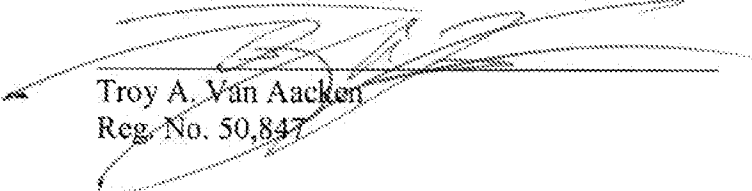
CONCLUSION

With this response, Assignee respectfully requests immediate allowance of pending claims. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: September 5, 2006

Fish & Richardson P.C.  
1230 Peachtree Street NE  
19th Floor  
Atlanta, GA 30309  
Telephone: (404) 892-5005  
Facsimile: (404) 892-5002



Troy A. Van Aacken  
Reg. No. 50,847